WHAT IS CLAIMED IS:

1. A watermark embedding process using a sub-band filtering, wherein original data are split into N×N blocks and then is transformed into frequency domain with N being not necessarily 8, and a HH band with N/2×N/2 coefficients is tested on a high frequency feature; the high frequency being recorded for watermark insertion; watermark data being transformed into frequency domain with full picture; LL-band coefficients being quantized and inserted into the HH band of a marked block of the original data ; a composite data of the original data and the watermark data being capable of being created by an inverse transformation of each block of the original data.

2. The watermark embedding process of Claim 1 further containing four keys for watermark extraction: (a) Privacy Key providing position of the marked blocks; (b) Permutation Function key decrypting random values into normal ones; (c) Quantization Table of $\tilde{\tilde{W}}_{LL}$: providing de-quantization for DCT coefficients of the watermark; (d) Embedding Coefficient Location extracting the watermark coefficient from HH band of the marked blocks; thus allowing the watermark to be extracted by means of first splitting the composite data into N×N blocks and transforming same to DCT domain ; the watermarking coefficients being capable of being extracted from the HH band of each block with system keys ; the watermark being then restored without using an original data ; the

watermark information being independent of the original data, allowing the system key to be pre-stored in the decoder.

3. A codebook based watermarking of the process of Claim 1, wherein the original data and watermark data all are transformed to frequency domain with full pictures, and the coefficient matrix of the original data are contents of the codebook; each watermarking coefficient being mapped to the codebook and inserted to the codebook; a best match being found and a coordinate thereof being recorded as the system key; the composite data being created from a modified codebook.

4. A composite system of the encryption and the watermark of the process as claimed in Claim 2, wherein the encryption is used to increase the security level and then watermarking process is used to hide the encrypted data; the key being encrypted and further watermarked by a second layer hidden; an encrypted bit of key being embedded to the LSB of the original data.

5. A JPEG processing of the watermark embedding process of Claim 4, wherein the bit of key is inserted to the LSB bit of non-zero DCT coefficient, and LL band of the watermark data for key information is scanned by a zigzag scan and a maximum weight scan to JPEG domain.

6. The watermark embedding process of Claim 1, wherein the watermark can be restored with only a certain degree of blurring but no serious distortion when the original data is under attack.

7. The watermark embedding process of Claim 1, wherein the watermark data include audio and video ones.

8. The watermark embedding process of Claim 1, wherein the watermark is gray-level data.

9. The watermark embedding process of Claim 1, wherein the watermark is binary data.

10. The watermark embedding process of Claim 1, wherein the transformation is not necessarily the DCT (discrete Cosine transform).